EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L23	115	(KOCHER near PAUL) (JAFFE near JOSHUA) (JUN near BENJAMIN) (CRYPTOGRAPHY NEAR RESEARCH)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:42
L24	61	23 and ((measur$5 study$3 analy$6 review$3 determin$7) near3 (attribut$3 radiat$3 electromagnetic power electric$3 voltage current noise signal$3 consum$6))	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:43
L25	10	24 and (command$3 signal$3 instructi$4) near3 (send$3 transmit$4)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:44

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	153	380/1	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 11:04
L5	23	4 and (measur$5 study$3 analy$6 review$3) near3 (attribut$3 radiat$3 electromagnetic power electric$3 voltage signal$3 consum$6)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 11:11
L6	4	5 and (command$3 signal$3 instructi$4 order$3) near3 (send$3 transmit$4)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 11:13

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	126860	"380"/$.ccls. "713"/$.ccls. "726"/$. ccls. "705"/$.ccls. "709"/$.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 11:30
L8	29647	7 and (measur$5 study$3 analy$6 review$3 determin$7) near3 (attribut$3 radiat$3 electromagnetic power electric$3 voltage current noise signal$3 consum$6)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:08
L9	13967	8 and (command$3 signal$3 instructi$4 order$3) near3 (send$3 transmit$4)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:10
L10	1872	9 and (attack$3 hack$3 tamper$3 criminal$4 unauthoriz$3 cryptoanaly$4 analysis) same (encrypt$3 cryptograph$5 cipher$3 scrambl$3)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:10
L13	31	10 and ((determin$6 measur$4 figur$3) near3 information near3 (key cryptograph$5))	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:11
L14	861065	(measur$5 study$3 analy$6 review$3 determin$7) near3 (attribut$3 radiat$3 electromagnetic power electric$3 voltage current noise signal$3 consum$6)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:09
L15	264159	14 and (command$3 signal$3 instructi$4) near3 (send$3 transmit$4)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:10
L16	3470	15 and (attack$3 hack$3 tamper$3 criminal$4 unauthoriz$3 cryptoanaly$4 analysis) same (encrypt$3 cryptograph$5 cipher$3 scrambl$3)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:10
L17	45	16 and ((determin$6 measur$4 figur$3) near3 information near3 (key cryptograph$5))	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 14:11

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L18	166	leak$3 near4 information near3 (key cryptograph$5)	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2006/09/19 14:22

L19	31	18 and ((determin$6 measur$4 figur$3) near4 information near3 (key cryptograph$5))	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2006/09/19 14:23

L20	17	19 and ((measur$5 study$3 analy$6 review$3 determin$7) near3 (attribut$3 radiat$3 electromagnetic power electric$3 voltage current noise signal$3 consum$6))	US-PGPUB;
			USPAT;
			USOCR
				OR	ON	2006/09/19 14:24

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L28	9	(INFORMATIOn and key and (measur$4 study$3 analy$4 review$3 determin$5) and (command$3 signal$3 instruct$3) and (cryptograph$5 encrypt$3 decrypt$3) and (attribut$3 radiat$3 electromagnetic power electric$3 voltage signal$3 current) and (device equipment) and operat$3 and (leak$3 dispers$3 dissipat$4 discover$3 reveal$3 disclos$3) and (statistic$4 pattern history probabl$4)).CLM.	US-PGPUB	OR	ON	2006/09/19 16:12

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	4	US-5136643-$.DID. OR US-5703413-$.DID. OR US-6236981-$.DID. OR US-6698662-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 16:49
S2	2	"6304658".pn. "6381699".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:16
S4	1	"5778065".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/12 19:14
S5	11	US-5017766-$.DID. OR US-5355413-$.DID. OR US-5495098-$.DID. OR US-5638444-$.DID. OR US-5696827-$.DID. OR US-5995624-$.DID. OR US-6115601-$.DID. OR US-6236981-$.DID. OR US-6289455-$.DID. OR US-6539092-$.DID. OR US-7073072-$.DID.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/19 11:03
S6	0	(US-5136643-$.DID. OR US-5703413-$.DID. OR US-6236981-$.DID. OR US-6698662-$.DID.) and ((attack$3 leak$3 compromis$3 hack$3))	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 16:56
S7	3	(US-5136643-$.DID. OR US-5703413-$.DID. OR US-6236981-$.DID. OR US-6698662-$.DID.) and (analog attribut$3 command radiati$3 power consum$3 convert$3 electromagnet$3)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:00
S8	2	"6304658".pn. "6278783".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:16
S9	6	(US-5017766-$.DID. OR US-5355413-$.DID. OR US-5495098-$.DID. OR US-5638444-$.DID. OR US-5696827-$.DID. OR US-5995624-$.DID. OR US-6115601-$.DID. OR US-6236981-$.DID. OR US-6289455-$.DID. OR US-6539092-$.DID. OR US-7073072-$.DID.) and (attack$3 leak$3 compromis$3 hack$3)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:32

EAST Search History

S10	10	(US-5017766-$.DID. OR US-5355413-$.DID. OR US-5495098-$.DID. OR US-5638444-$.DID. OR US-5696827-$.DID. OR US-5995624-$.DID. OR US-6115601-$.DID. OR US-6236981-$.DID. OR US-6289455-$.DID. OR US-6539092-$.DID. OR US-7073072-$.DID.) and (analog attribut$3 command radiati$3 power consum$3 convert$3 electromagnet$3)	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:42
S11	6	S9 and S10	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:33
S12	10	S9 S10	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:33
S13	4	S10 and command$3	US-PGPUB; USPAT; USOCR	OR	ON	2006/09/18 17:43

Terms used **command sequence key information leaking cryptographic operation measuring**

Found **3** of **185,178**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 3 of 3

Relevance scale

1 Strength of two data encryption standard implementations under timing attacks
Alejandro Hevia, Marcos Kiwi
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press
Full text available: pdf(183.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study the vulnerability of two implementations of the Data Encryption Standard (DES) cryptosystem under a timing attack. A timing attack is a method, recently proposed by Paul Kocher, that is designed to break cryptographic systems. It exploits the engineering aspects involved in the implementation of cryptosystems and might succeed even against cryptosys-tems that remain impervious to sophisticated cryptanalytic techniques. A timing attack is, essentially, a way of obtaining some users ...

Keywords: cryptanalysis, cryptography, data encryption standard, timing attack

2 Practical byzantine fault tolerance and proactive recovery
Miguel Castro, Barbara Liskov
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Our growing reliance on online services accessible on the Internet demands highly available systems that provide correct service without interruptions. Software bugs, operator mistakes, and malicious attacks are a major cause of service interruptions and they can cause arbitrary behavior, that is, Byzantine faults. This article describes a new replication algorithm, BFT, that can be used to build highly available systems that tolerate Byzantine faults. BFT can be used in practice to implement re ...

Keywords: Byzantine fault tolerance, asynchronous systems, proactive recovery, state machine replication, state transfer

Ravi Sandhu, Xinwen Zhang
June 2005 **Proceedings of the tenth ACM symposium on Access control models and technologies**
Publisher: ACM Press
Full text available: pdf(215.48 KB) Additional Information: full citation, abstract, references, index terms

It has been recognized for some time that software alone does not provide an adequate foundation for building a high-assurance trusted platform. The emergence of industry-standard trusted computing technologies promises a revolution in this respect by providing roots of trust upon which secure applications can be developed. These technologies offer a particularly attractive platform for security in peer-to-peer environments. In this paper we propose a trusted computing architecture to enforce ac ...

Keywords: access control, policy enforcement, security architecture, trusted computing

Results 1 - 3 of 3

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player